UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of: Information associated with accounts identified as offthejugg_805 and emiliovelci11 that is within the possession, custody, or control of Snap Inc.	)	Case No.2:22-MJ-2684

APPLICATION FOR WARRANT BY TELEPHONE PURSUANT TO 18 U.S.C. § 2703

I, a federal law enforcement officer, request a warrant pursuant to Title 18, United States Code, Section 2703, and state under penalty of perjury that I have reason to believe that within the following data:

See Attachment A

There are now concealed or contained the items described below:

See Attachment B

The basis for the search is:

☑ Evidence of a crime;
☑ Contraband, fruits of crime, or other items illegally possessed;
☐ Property designed for use, intended for use, or used in committing a crime.

The search is related to a violation of:

Code section(s)	*Offense Description*
21 U.S.C. §§ 841(a)(1), 846	See attached affidavit

The application is based on these facts:

See attached Affidavit, which is incorporated herein by reference.

/s/ Gabriel Perez
Applicant's signature
Gabriel Perez, DEA Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

City and State: _____

Hon. John E. McDermott, U.S. Magistrate Judge
Printed name and title

AUSA: Julia Hu (x3802)

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the Instagram accounts identified as offthejugg_805 ("SUBJECT ACCOUNT 1") and emiliovelci11 ("SUBJECT ACCOUNT 2") (collectively, the "SUBJECT ACCOUNTS"), that is within the possession, custody, or control of Snap Inc., a company that accepts service of legal process at 2772 Donald Douglas Loop North, Santa Monica, CA 90405, regardless of where such information is stored, held, or maintained.

ATTACHMENT B

ITEMS TO BE SEIZED

I. SEARCH PROCEDURE

1. The warrant will be presented to personnel of Snap Inc. (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below in Section IV.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.10.a. below), law enforcement agents and/or individuals assisting law enforcement and acting at their direction (the "search team") will examine such content records pursuant to search procedures specifically designed to identify items to be seized under this warrant. The search shall extract and seize only the specific items to be seized under this warrant (see Section III below). The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

5. If the search team encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

6. The search team will complete its search of the content records as soon as is practicable but not to exceed 120 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the content records beyond this 120-day period without first obtaining an extension of time order from the Court.

7. Once the search team has completed its review of the content records and created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the search team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, the search team will not access the data from the sealed original production which fell outside the scope of the items to be seized absent further order of the Court.

8. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

9. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

10. To the extent that the information described in Attachment A is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each SUBJECT ACCOUNT listed in Attachment A:

a. All contents of all wire and electronic communications associated with the SUBJECT ACCOUNT, limited to that which occurred on or after January 1, 2020, including:

i. All e-mails, communications, or messages of any kind associated with the SUBJECT ACCOUNT, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information associated with each e-mail or message, and any related documents or attachments.

ii. All records or other information stored by subscriber(s) of the SUBJECT ACCOUNT, including address books, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files.

iii. All data and information associated with the profile page of the SUBJECT ACCOUNT, including photographs, "bios," and profile backgrounds and themes;

iv. All communications or other messages sent or received by the SUBJECT ACCOUNT, including via Instagram Direct;

v. All user content created, uploaded, or shared by the SUBJECT ACCOUNT, including any comments made by the SUBJECT ACCOUNT on photographs, videos, or other content;

vi. All photographs, videos, images, comments, captions, and hashtags, as well as any metadata associated therewith, in the user gallery for the SUBJECT ACCOUNT;

vii. All location data associated with the SUBJECT ACCOUNT, or with photographs, videos, or other content, including geotags;

viii. All records of Snapchat searches performed by the SUBJECT ACCOUNT, including all past searches saved by the SUBJECT ACCOUNT;

ix. A list of all of the people that the user of the SUBJECT ACCOUNT follows on Snapchat and all people who are following the user (i.e., the user's "following" list and "followers" list), as well as any "friends" of the user;

x. A list of all users that the SUBJECT ACCOUNT has "unfollowed" or blocked;

xi. All records pertaining to communications between the PROVIDER and any person regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, and including any changes made to any subscriber information or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the following accounts:

(I) the SUBJECT ACCOUNTS.

ii. All user connection logs and transactional information of all activity relating to the SUBJECT ACCOUNTS described above in Section II.10.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations, and including specifically the specific product name or service to which the connection was made.

iii. All privacy and account settings of the SUBJECT ACCOUNTS, including past and present account status.

iv. All information about connections between the SUBJECT ACCOUNTS and third-party websites and applications.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

11. For each SUBJECT ACCOUNT listed in Attachment A, the search team may seize:

a. All information described above in Section II.10.a that constitutes evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (distribution of and possession with intent to distribute and distribution of controlled substances) and 21 U.S.C. § 846 (attempt and conspiracy to possess with intent to distribute and distribute controlled substances) (the "SUBJECT OFFENSES"), namely:

i. Information relating to who created, accessed, or used the SUBJECT ACCOUNT, including records about their identities and whereabouts.

ii. Information and any communications relating to the purchase, sale, distribution, transportation, and/or possession of drugs;

iii. Information reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of controlled substances, or drug customers, including calendars, address books, telephone or other contact lists, pay/owe records, distribution or customer lists, correspondence,

receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed;

iv. Information relating to the location, storage, or concealment of cash, money instruments, virtual currency, or money equivalents;

v. Information relating to co-conspirators engaged in the SUBJECT OFFENSES, which could include information relating to their identities, whereabouts, communications, and methods of contact and communication; and

vi. Evidence indicating the state of mind as it relates to the crimes under investigation.

b. Files, databases, and database records stored by the PROVIDER on behalf of the subscriber or user operating the SUBJECT ACCOUNTS, including:

i. e-mail accounts and the contents thereof, associated with the account.

c. Subscriber information related to the accounts enumerated in Attachment A, to include:

i. Names, physical addresses, telephone numbers and other identifiers, e-mail addresses, and business information;

ii. Length of service (including start date), types of service utilized, means and source of payment for services (including any credit card or back account number), and billing and payment information;

iii. Any information showing the location of the users of the SUBJECT ACCOUNTS, including while sending or receiving a message using the SUBJECT ACCOUNTS or accessing or logged into the SUBJECT ACCOUNTS, as well any associated accounts; and

c. All records and information described above in Section II.10.b.

IV. PROVIDER PROCEDURES

11. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. The PROVIDER shall send such information to:

DEA Special Agent Gabriel Perez
Department of Justice/Drug Enforcement Administration
770 Paseo Camarillo #300
Camarillo, CA 93010
213-725-3865
Gabriel.X.Perez@USDOJ.GOV

12. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

13. IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 2705(b), that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A, of the existence of the warrant, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date this warrant is signed by the magistrate judge or such later date as may be set by the

Court upon application for an extension by the United States. Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the PROVIDER shall notify the agent identified above of its intent to so notify.

AFFIDAVIT

I, Gabriel Perez, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Drug Enforcement Administration ("DEA"), and have been so employed since July 2012. I am currently assigned to the Ventura Resident Office ("VRO"), in Camarillo, California.

2. Upon joining the DEA, I attended and graduated from the sixteen-week DEA Basic Agent Training in Quantico, Virginia. During the training, I received several hundred hours of comprehensive, formalized instruction on such matters as drug identification, detection, and interdiction, drug enforcement laws, surveillance techniques, informant handling, interviewing, report writing, money laundering techniques, and asset identification, seizure, and forfeiture. I have also completed a field-training program under the direction of a senior agent and have spent numerous hours working with senior special agents conducting complex drug investigations. Additionally, I have attended special training in wire and electronic interceptions and the use of wire and electronic equipment.

3. During my employment with DEA, I have participated in drug investigations as both a case agent and in a supportive role. I have assisted in the arrest of multiple drug traffickers as a result of these investigations. I have witnessed and assisted other officers and agents interview informants and suspects concerning the methods and means of drug

traffickers. I have participated in several static and mobile surveillance activities across Southern California and have assisted in the execution of multiple search warrants.

4. Through these investigations, my training and experience, and conversations with other agents and law enforcement personnel, both in the United States and elsewhere, I have become familiar with the methods used by narcotics traffickers to smuggle and safeguard narcotics, to distribute narcotics, and to collect and launder proceeds related to the sales of narcotics.

5. Additionally, I have received training and have gained first-hand knowledge on the diversion of controlled substance pharmaceuticals. I have attended intelligence meetings and received intelligence briefs on the prevalent abuse of prescription drugs in society today. I have also spoken with experienced DEA diversion investigators concerning the methods and practices of criminals who are engaged in the illegal trade of prescription medication.

6. In my duties as a DEA SA, I also have been specially trained in the use of court-ordered interceptions of wire and electronic communications. I was also instructed in the use of wire and electronic communications interception as a tool to disrupt and dismantle drug trafficking organizations.

7. I make this affidavit in support of an application for a warrant for information associated with the accounts identified as offthejugg_805 ("SUBJECT ACCOUNT 1") and emiliovelci11 ("SUBJECT ACCOUNT 2") (collectively, the "SUBJECT

ACCOUNTS") that is stored at premises controlled by Snap Inc. (the "PROVIDER"), a provider of electronic communication and remote computing services, headquartered at 2772 Donald Douglas Loop North, Santa Monica, CA 90405.[1] The information to be searched is described in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A) and 2703(d)[2] to require the PROVIDER to disclose to the government copies of the information (including the content of communications) described

---

[1] Because this Court has jurisdiction over the offenses being investigated, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). See 18 U.S.C. §§ 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction") and 2711 ("the term 'court of competent jurisdiction' includes -- (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that -- (i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title").

[2] The government is seeking non-content records pursuant to 18 U.S.C. § 2703(d). To obtain the basic subscriber information, which does not contain content, the government needs only a subpoena. See 18 U.S.C. § 2703(c)(1), (c)(2). To obtain additional records and other information--but not content--pertaining to subscribers of an electronic communications service or remote computing service, the government must comply with the dictates of section 2703(c)(1)(B), which requires the government to supply specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation in order to obtain an order pursuant to 18 U.S.C. § 2703(d). The requested warrant calls for both records containing content (see Attachment B paragraph II.10.a.) as well as subscriber records and other records and information that do not contain content (see Attachment B paragraph II.10.b.).

in Section II of Attachment B. Upon receipt of the information described in Section II of Attachment B, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items described in Section III of Attachment B. Attachments A and B are incorporated herein by reference.

8. As described more fully below, I respectfully submit there is probable cause to believe that the information associated with the SUBJECT ACCOUNTS constitutes evidence, contraband, fruits, or instrumentalities of criminal violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute and distribution of controlled substances) and 21 U.S.C. § 846 (conspiracy to possess with intent to distribute and distribute controlled substances) (the "SUBJECT OFFENSES").

9. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, and all dates are approximate.

II. SUMMARY OF PROBABLE CAUSE

10. On March 9, 2020, E.V. ("Decedent") died from a fentanyl overdose in his residence in Atascadero, California.

On a table next to Decedent was an Apple iPhone 8 ("Device 2"), which Decedent's brother, M.V., confirmed belonged to Decedent.

11. According to M.V., the previous day, he had driven Decedent in his car to a restaurant in Paso Robles, California, where Decedent bought three blue M-30 pills from an individual later identified as TIMOTHY CLARK WOLFE ("WOLFE"). Surveillance video shows WOLFE exiting the restaurant and getting into M.V.'s car. On the way home, Decedent took one of the pills.

12. In M.V.'s car on March 9, 2020, officers found a plastic bag containing two blue M-30 pills. Lab testing confirmed that both pills contained fentanyl. An autopsy report confirmed that Decedent died from fentanyl intoxication, and a toxicology report confirmed that fentanyl was present in Decedent's system.

13. On March 9, 2020, Atascadero Police Department ("APD") officers seized an Apple iPhone 7 Plus ("Device 1") from WOLFE's person.

14. A search of Device 1 showed that WOLFE was signed into Snapchat as SUBJECT ACCOUNT 1. There were multiple communications on Snapchat between SUBJECT ACCOUNT 1 and individuals related to sale of drugs.

15. A search of Device 2 showed that Decedent was signed into Snapchat as SUBJECT ACCOUNT 2. On March 8, 2020, shortly before the fentanyl transaction between Decedent and WOLFE, there were two Snapchat voice calls from SUBJECT ACCOUNT 1 to SUBJECT ACCOUNT 2. In addition, SUBJECT ACCOUNT 1 sent SUBJECT

ACCOUNT 2 a Snapchat message around the time of the fentanyl transaction.

III. STATEMENT OF PROBABLE CAUSE

16. Based on my review of law enforcement reports, conversations with other law enforcement agents, my review of cell phone extraction reports, and my own knowledge of the investigation, I am aware of the following:

A. Investigation of the Fentanyl Overdose Death of E.V.

1. APD Found E.V. Dead at the Garcero Road Residence on March 9, 2020

17. Based on my review of APD reports and bodycam recordings and my conversations with law enforcement agents, I know the following.

18. On March 9, 2020, APD and Atascadero Fire Department units went to a house on Garcero Road in Atascadero, California in response to a 911 call from M.V. According to M.V., his 19-year-old brother, Decedent, had taken an unknown pill the night before and was not waking up.

19. Officers found E.V. in the living room, lying on his back next to the couch, cold to the touch, with foam emitting from his nostrils and mouth. Atascadero Fire Department units pronounced Decedent dead at 8:08 a.m.

20. Device 2 was on the table next to Decedent, which was taken into APD custody. M.V. confirmed that Device 2 belonged to Decedent.

21. Officers found a small glass vial with white powder residue on the ground near Decedent's feet. Subsequent lab

testing confirmed that the residue contained Methylenedioxymethamphetamine ("MDMA").

22. APD Officer Steven Stucky spoke with M.V. at the scene. M.V. stated that he was present with Decedent on March 8, 2020, when Decedent purchased three pills from "Tim," later identified as WOLFE, at Les Petites Canailles, a restaurant in Paso Robles, California. M.V. stated that Decedent was in M.V.'s vehicle at the time of this transaction and he saw Decedent take one of the three pills.

2. Officers Found Two Fentanyl Pills in M.V.'s Car

23. Based on my review of APD reports and bodycam recordings and my conversations with law enforcement agents, I know the following.

24. On March 9, 2020, Officer Stucky obtained verbal consent from M.V. to search the inside of M.V.'s dark grey Toyota Prius, bearing California license plate number 8KOJ561.

25. According to M.V., Decedent was seated in the front passenger seat when the March 8, 2020, drug transaction with WOLFE occurred.

26. On the front passenger floorboard, Officer Stucky found a plastic baggie which contained two blue pills, each stamped with "M" and the number "30." Subsequent lab testing confirmed that both pills contained fentanyl.

27. M.V. told Officer Stucky that the baggie found in his car was the same one that Decedent had purchased from "Tim" and left in his car.

3. Interview of M.V.

28. APD Detective Samuel Rodriguez conducted a recorded interview with M.V. on March 9, 2020. Based on my review of the interview recording, I know that M.V. told Detective Rodriguez the following:

a. M.V. and Decedent went to lunch in Paso Robles at approximately 3:00 p.m.

b. M.V. stated that during lunch, Decedent began messaging on Decedent's phone, Device 2, with a person named "Tim" to arrange for the purchase of Percocet pills from him.

c. M.V. noted that he believed Decedent was using wireless internet at the restaurant to message WOLFE through a messaging application, as Decedent's phone did not have cellular service.

d. M.V. agreed to drive Decedent to Les Petites Canailles restaurant in Paso Robles to meet with WOLFE.

e. M.V. and Decedent arrived at the rear of the building at approximately 6:00 p.m.

f. WOLFE got into the back seat of M.V.'s vehicle and gave Decedent a plastic baggie containing three small blue pills, for which Decedent paid approximately $30.

g. WOLFE told Decedent to "[l]et me know if you need anymore, I have a lot," as he exited M.V.'s vehicle.

h. On the drive home, Decedent opened the baggie that he got from WOLFE and asked M.V. for water. M.V. observed Decedent swallow what he believed to be one of the three pills.

i. M.V stated that he and Decedent went home and watched a movie, during which Decedent "passed out" at approximately 8:00 p.m. M.V. went to his room to go to bed at approximately midnight, checking on Decedent and making sure Decedent was still breathing with a pulse before doing so.

j. M.V. woke up on March 9, 2020, to one of their roommates, J.L., yelling for help. M.V. stated that they called 9-1-1 and awaited EMS.

B. Identification of WOLFE as the Seller of the Fentanyl Pills to Decedent

29. Based on my review of APD reports and my conversations with law enforcement agents, I know the following.

30. On March 9, 2020, Detective Rodriguez spoke to the owners of the Les Petites Canailles restaurant, C.A. and J.A.

a. According to C.A. and J.A., they were aware of Decedent's death and that another employee, WOLFE, had sold prescription medication to Decedent.

b. C.A. and J.A. stated that they had reviewed video surveillance from the rear of their restaurant and had seen WOLFE step outside several times throughout the evening of March 8, 2020.

c. J.A. provided WOLFE's cell phone number as 805-423-2160, which is tied to Device 1.

31. APD officers obtained the surveillance video footage from the Les Petites Canailles restaurant for March 8, 2020. The video, which I have reviewed, shows the following:

a. At approximately 6:46 p.m., WOLFE came out of the rear door of the restaurant and walked out of the camera view to the right of the frame.

b. Approximately 15 seconds later, the video captures the sound of a car door shutting.

c. At approximately 6:47 p.m., the video captures the sound of a car door opening and closing.

d. WOLFE then reenters the frame of the camera.

e. As WOLFE returns to the restaurant through the rear door, a dark gray Toyota Prius drives away. The car matches M.V.'s car from which the two fentanyl pills were seized on March 9, 2020.

32. APD officers also obtained surveillance video footage from a City of Paso Robles public safety camera in a public parking lot at the corner of 12th Street and Spring Street, which had a view of the rear parking lot of Les Petites Canailles. The video, which I have reviewed, shows the following:

a. At approximately 6:45 p.m., WOLFE exited the rear of Les Petites Canailles and walked over to a dark gray Toyota Prius, matching M.V.'s, that was parked in the parking lot.

b. WOLFE got into the Prius through the rear passenger side door and stayed in the car for less than one minute.

c. WOLFE then got out of the Prius and ran back into the rear door of the restaurant.

d. The Prius then pulled out of the parking lot and drove off.

C. Execution of Search Warrant for WOLFE's Residence

33. Based on my review of APD reports, search warrants, and photographs and my conversations with law enforcement agents, I know the following.

34. On March 9, 2020, the Honorable Gayle Peron, County of San Luis Obispo Superior Court Magistrate Judge, signed a search warrant for Decedent's cellular phone, Device 2. In that same warrant, Judge Peron also authorized a search of WOLFE's residence on Flag Way in Paso Robles, California, WOLFE's person, and any cellular devices recovered from WOLFE or his residence.

35. On March 9, 2020, APD officers executed the search warrant for WOLFE's residence, where he lived with his sister, T.W., and her partner, J.I. WOLFE was not present at the location at the time of the warrant, but T.W. and J.I. were.

36. T.W. identified WOLFE's bedroom to APD officers. The bedroom appeared to belong to WOLFE based on the fact that it contained mail addressed to WOLFE and other personal effects. Officers searched WOLFE's bedroom and found the following:

a. A backpack containing numerous white prescription pills and a digital scale. Subsequent lab testing confirmed that the pills were Alprazolam, Baclofen, and Promethazine.

b. One additional cell phone and a Macbook Pro; and

c. A change of address validation for Wolfe, showing the Flag Way residence as his registered address.

D. Arrest and Interview of WOLFE

37. Based on my review of audio and video recordings of the below-described interview and APD reports, I know the following.

38. On March 9, 2020, APD officers found WOLFE at a Chili's restaurant in Paso Robles, California. Pursuant to the search warrant, officers searched WOLFE and recovered Device 1 from his person.

39. APD Detective Rodriguez advised WOLFE of his Miranda rights, and WOLFE agreed to be interviewed. WOLFE initially admitted to facilitating a transaction between his "plug" and Decedent for $75 on March 8, 2020, but stated that he did not physically hand Decedent the pills.

40. After WOLFE requested that the interview continue at APD, APD officers transported WOLFE to the APD Station. Once at the station, Detective Rodriguez reminded WOLFE of his Miranda rights, and WOLFE agreed to continue speaking to Detective Rodriguez. WOLFE told Detective Rodriguez the following:

a. WOLFE stated that the pills seized from the backpack in his room were Xanax and Promethazine.

b. WOLFE continued to state that he was simply a middleman and had not physically provided the pills to Decedent on March 8, 2020.

c. When confronted with the witness statement from M.V., WOLFE admitted to handing Decedent the baggie of pills and collecting $75 in exchange.

d. WOLFE stated that he had given Decedent his Snapchat username a few days prior to the transaction with Decedent.

e. WOLFE stated that he originally obtained the pills from his source for $35 and sold them at a high markup to Decedent because he believed him to be naïve regarding opioids.

E. Autopsy and Toxicology Results

41. On April 15, 2020, Dr. Joye M. Carter M.D. of the San Luis Obispo County Sheriff-Coroner issued the final autopsy report for Decedent. The report identified the cause of death as "complications of fentanyl intoxication."

42. A toxicology report issued by Central Valley Toxicology, Inc. determined that fentanyl was present in Decedent's system at a concentration of 0.015 mg/L. As stated in the report, the potentially toxic range for fentanyl is between 0.003 and 0.010 mg/L. Tetrahydrocannabinol ("THC") metabolites were also present in Decedent's system, indicating recent marijuana use, but no other drugs were detected.

F. During a Search of Devices 1 and 2, Agents Find Snapchat Messages Tied to SUBJECT ACCOUNTS 1 and 2

43. On March 10, 2020, pursuant to the state search warrant, APD Technician Enfantino conducted forensic extractions of Devices 1 and 2.

44. On April 20, 2022, the Honorable Jean Rosenbluth, United States Magistrate Judge, issued search warrants for Devices 1 and 2. Case No. 22-MJ-1580.

45. Pursuant to the federal search warrant, DEA agents have reviewed the extractions reports for Devices 1 and 2.

46. Although I describe the relevant Snapchat communications found on Devices 1 and 2 below, I know from my training and experience and conversations with other law enforcement agents that electronic devices do not always retain all communications sent or received by the user through the Snapchat application, depending on the user's settings. Although messages may be erased from a user's phone, it is possible that Snapchat still keeps a record of the communications.

1. Device 1 Contains Drug-Related Snapchat Communications Linked to SUBJECT ACCOUNT 1

47. Based on my review of the extraction report for Device 1, I know the following.

48. WOLFE was signed into Snapchat on Device 1 as SUBJECT ACCOUNT 1. The name connected to SUBJECT ACCOUNT 1 was "OTX TDubb." Based on my training and experience, I know that "OTX" stands for "Off the Xan," which indicates that someone is high on Xanax, a Schedule IV controlled substance.

49. On March 5, 2020, SUBJECT ACCOUNT 1 added SUBJECT ACCOUNT 2 as a contact in Device 2.

50. SUBJECT ACCOUNT 1 last contacted SUBJECT ACCOUNT 2 on March 8, 2020, at 6:47 p.m.

51. Device 1 contained communications on Snapchat between WOLFE using SUBJECT ACCOUNT 1 and other individuals related to sale of drugs. For example:

a. On March 8, 2020, SUBJECT ACCOUNT 1 sent a message to a Snapchat group thread, "I need a delivery tonight for buds around 10-10:30 who got me." Based on my training and experience and knowledge of the investigation, I know that "bud" refers to marijuana, a Schedule I controlled substance.

b. On March 9, 2020, SUBJECT ACCOUNT 1 was part of two different Snapchat conversations where pictures of marijuana were displayed. Based on my training and experience, I know that individuals selling controlled substances will display their respective products for sale prospective customers.

2. Device 2 Contains Communications Between SUBJECT ACCOUNT 1 and SUBJECT ACCOUNT 2

52. Based on my review of the extraction report for Device 2, I know the following.

53. Decedent was signed into Snapchat on Device 2 as SUBJECT ACCOUNT 2.

54. On March 5, 2020, Decedent added SUBJECT ACCOUNT 1 as a contact.

55. On March 8, 2020, there were two incoming Snapchat voice calls from SUBJECT ACCOUNT 1 to SUBJECT ACCOUNT 2 at approximately 4:19 p.m. and 4:22 p.m.[3]

[3] In the affidavit in support of a search warrant for Devices 1 and 2, SA Robert Thomas stated that Detective Rodriguez had reviewed the extraction report for Device 2 and that there were Instagram voice calls between WOLFE and Decedent. However, that was based on Detective Rodriguez's representation in a police report that SA Thomas reviewed. Upon SA Thomas's review of the extraction report for Device 1, SA Thomas determined that the voice calls at 4:19 p.m. and 4:22 p.m. on March 8, 2020, were actually on Snapchat from SUBJECT ACCOUNT 1 to SUBJECT ACCOUNT 2.

a. Those calls took place only a few hours before surveillance video shows WOLFE getting into M.V.'s car for the fentanyl transaction on March 8, 2020.

b. Based on my training and experience, I know that drug dealers often communicate with their customers through phone calls or calls on social media applications to avoid creating a written record of the transaction.

56. On March 8, 2020, at 6:47 p.m., there was a Snapchat message sent from SUBJECT ACCOUNT 1 to SUBJECT ACCOUNT 2. The extraction report for Device 2 shows that this was the last time that SUBJECT ACCOUNT 1 contacted SUBJECT ACCOUNT 2. However, the content of the message is not available from the extraction report. According to a DEA forensic expert, depending on a particular user's phone settings, Snapchat messages may disappear from the phone after being opened.

G. Prior State Search Warrant for SUBJECT ACCOUNT 1

57. On September 30, 2020, the Honorable Jesse J. Marino, County of San Luis Obispo Superior Court Magistrate Judge, signed a search warrant for Snapchat subscriber information and messages, photos, and logs for SUBJECT ACCOUNT 1 for the period of May 30, 2019, to September 30, 2020.

58. Pursuant to the search warrant, APD Detective Rodriguez received records from Snapchat on November 19, 2020. The phone number associated with SUBJECT ACCOUNT 1 was the 3689 number, which matches Device 1.

59. Detective Rodriguez reviewed the conversation history, which included only one group chat dated June 19, 2019, between

SUBJECT ACCOUNT 1 and users "valentina_11" and "isaac_2bomb." In the chat, WOLFE mentions getting "norcos" as a treatment for strep throat.

H. Preservation of SUBJECT ACCOUNT 2

60. On July 6, 2022, SA Robert Thomas spoke with a legal representative from Snapchat, who stated that Snapchat currently still has records pertaining to SUBJECT ACCOUNT 2 in their systems. SA Thomas did not inquire about SUBJECT ACCOUNT 1.

IV. BACKGROUND ON SOCIAL MEDIA ACCOUNTS AND THE PROVIDER

61. In my training and experience, I have learned that providers of social media services offer a variety of online services to the public. Providers, like the PROVIDER, allow subscribers to obtain accounts like the SUBJECT ACCOUNTS. Subscribers obtain an account by registering with the provider. During the registration process, providers generally ask their subscribers to provide certain personal identifying information when registering for an email or social media account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Some providers also maintain a record of changes that are made to the information provided in subscriber records, such as to any other email addresses or phone numbers supplied in subscriber records. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of an account.

62. Therefore, the computers of the PROVIDER are likely to contain stored electronic communications and information concerning subscribers and their use of the PROVIDER's services, such as account access information, email or message transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of a SUBJECT ACCOUNT.

63. A subscriber of the PROVIDER can also store with the PROVIDER files in addition to emails or other messages, such as address books, contact or buddy lists, groups, social network links, calendar data, pictures or videos (other than ones attached to emails), notes, and other files, on servers maintained and/or owned by the PROVIDER. In my training and experience, evidence of who was using an account may be found in such information.

64. In my training and experience, email and social media providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email

and social media providers often have records of the Internet Protocol ("IP") address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a SUBJECT ACCOUNT.

65. In my training and experience, email and social media account users will sometimes communicate directly with the service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers of emails and social media services typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of a SUBJECT ACCOUNT.

V. BACKGROUND ON THE SEIZURE OF DIGITAL EVIDENCE FROM THE PROVIDER

66. I know from my training and experience that the complete contents of an account may be important to establishing the actual user who has dominion and control of that account at a given time. Accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by

multiple people. Given the ease with which accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an account, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces will come from a time period before the account was used in the criminal activity. Limiting the scope of the search would, in some instances, prevent the government from identifying the true user of the account and, in other instances, may not provide a defendant with sufficient information to identify other users of the account. Therefore, the contents of a given account, including the email addresses or account identifiers and messages sent to that account, often provides important evidence regarding the actual user's dominion and control of that account. For the purpose of searching for content demonstrating the actual user(s) of a SUBJECT ACCOUNT, I am requesting a warrant requiring the PROVIDER to turn over all information associated with a SUBJECT ACCOUNT with the date restriction included in Attachment B for review by the search team.

67. Relatedly, the government must be allowed to determine whether other individuals had access to a SUBJECT ACCOUNT. If the government were constrained to review only a small subsection of an account, that small subsection might give the

misleading impression that only a single user had access to the account.

68. I also know based on my training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as "lol" to express "laugh out loud"), or codewords (which require entire strings or series of conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of a message or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and parenthesis :) to convey a smile or agreement) to discuss matters. "Keyword searches" would not account for any of these possibilities, so actual review of the contents of an account by law enforcement personnel with information regarding the identified criminal activity, subject to the search procedures set forth in Attachment B, is necessary to find all relevant evidence within the account.

69. This application seeks a warrant to search all responsive records and information under the control of the PROVIDER, which is subject to the jurisdiction of this court, regardless of where the PROVIDER has chosen to store such information.

70. As set forth in Attachment B, I am requesting a warrant that permits the search team to keep the original production from the PROVIDER, under seal, until the investigation is completed and, if a case is brought, that case is completed through disposition, trial, appeal, or collateral proceeding.

a. I make that request because I believe it might be impossible for a provider to authenticate information taken from a SUBJECT ACCOUNT as its business record without the original production to examine. Even if the provider kept an original copy at the time of production (against which it could compare against the results of the search at the time of trial), the government cannot compel the provider to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the provider to examine a particular document found by the search team and confirm that it was a business record of the provider taken from a SUBJECT ACCOUNT.

b. I also know from my training and experience that many accounts are purged as part of the ordinary course of business by providers. For example, if an account is not accessed within a specified time period, it -- and its contents -- may be deleted. As a consequence, there is a risk that the only record of the contents of an account might be the production that a provider makes to the government, for example, if a defendant is incarcerated and does not (perhaps cannot) access his or her account. Preserving evidence, therefore,

would ensure that the government can satisfy its Brady obligations and give the defendant access to evidence that might be used in his or her defense.

VI. REQUEST FOR NON-DISCLOSURE

71. Pursuant to 18 U.S.C. § 2705(b), I request that the Court enter an order commanding the PROVIDER not to notify any person, including the subscribers of the SUBJECT ACCOUNTS, of the existence of the warrant until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the requested warrant is signed by the magistrate judge, or such later date as may be set by the Court upon application for an extension by the United States. There is reason to believe that such notification will result in: (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; (5) otherwise seriously jeopardizing the investigation; or (6) unduly delaying trial. The current investigation set forth above is not public, and I know, based on my training and experience, that individuals engaged in drug trafficking often will destroy digital evidence if they learn of an investigation. In addition, if the PROVIDER or other person notifies the target of the investigation that a warrant has been issued for a SUBJECT ACCOUNTS, the individual might further mask their activity, or delete additional accounts, and seriously jeopardize the investigation.

VII. CONCLUSION

72. Based on the foregoing, I request that the Court issue the requested warrant. The government will execute this warrant by serving the warrant on the PROVIDER. Because the warrant will be served on the PROVIDER, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ____ day of July, 2022.

_____

HONORABLE JOHN MCDERMOTT
UNITED STATES MAGISTRATE JUDGE